UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,017	03/18/2004	Wilson Sing-Hei So	36992.00107 (HAL 265)	7773

44955 7590 01/06/2009
SQUIRE, SANDERS & DEMPSEY L.L.P.
1 MARITIME PLAZA, SUITE 300
SAN FRANCISCO, CA 94111

EXAMINER	
JOHNS, CHRISTOPHER C	
ART UNIT	PAPER NUMBER
3621	
MAIL DATE	DELIVERY MODE
01/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/805,017	SO ET AL.	
	Examiner	Art Unit	
	Christopher C. Johns	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6,8-15,18,19 and 21-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6,8-15,18,19 and 21-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 C.F.R. §1.114

1. A request for continued examination under 37 C.F.R. § 1.114, including the fee set forth in 37 C.F.R. § 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 C.F.R. §1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 C.F.R. §1.114. Applicant's submission filed on 25 September 2008 has been entered.

Acknowledgements

2. Claims 1-4, 6, 8-15, 18, 19, and 21-24 are pending.

Claim Objections

3. Claims 1-4, 6, 8-11, 21, and 23 are objected to for usage of the functional language "for (action)". It is believed that Applicants intend "for (action)" to mean "programmed to" since "for" is functional language and therefore given less patentable weight[1]. In light of the notice function of the claims, the Examiner respectfully requests changing "for (action)" to "programmed to (perform an action)" where a positive recitation is desired[2].

---

[1] As it is written, the Examiner interprets the claim as follows: "a first site coupled to a network, a terminal coupled to the network, a second site coupled to the network…the terminal having logic, logic, and logic, the second site having logic, wherein a list containing information is sent from the first site to the terminal". Note that the final limitation ("wherein a list containing…") of the independent claim is almost entirely non-functional descriptive material and as such, is not sufficient to distinguish the claimed invention from the prior art. Nevertheless, in the interest of compact prosecution, the Examiner has performed a search, and applied the prior art as if the "list" were statutorily sufficient to distinguish from the prior art. See MPEP §2106.01.

[2] See MPEP §2114 - "While features of an apparatus may be recited either structurally or functionally, claims

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-4, 6, 8-11, 21, and 23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Independent claim notes that "the secure device provides the terminal with the encrypted personal data and the first key to the terminal". It is believed that this is a typographical error, as there is no "key to the terminal" - rather, it is believed that Applicants are attempting to claim "providing…the encrypted personal data and the first key to the terminal".

7. As it is written, the claim is rendered indefinite because it is not clear what key is being sent, as there is no "key to the terminal".

8. Dependent claims 2-4, 6, 8-11, 21, and 23 are all rejected for at least their dependency upon claim 1.

---

directed to an apparatus must be distinguished from the prior art in terms of structure rather than function" (emphasis mine). The Manual then cites important precedent: "In re Schreiber, 128 F.3d 1473, 1477-78, 44 USPQ2d 1429, 1431-32 (Fed. Cir. 1997) (The absence of a disclosure in a prior art reference relating to function did not defeat the Board's finding of anticipation of claimed apparatus because the limitations at issue were found to be inherent in the prior art reference); see also In re Swinehart, 439 F.2d 210, 212-13, 169 USPQ 226, 228-29 (CCPA 1971); In re Danly, 263 F.2d 844, 847, 120 USPQ 528, 531 (CCPA 1959). "Apparatus claims cover what a device is, not what a device does." Hewlett-Packard Co. v. Bausch & Lomb Inc., 909 F.2d 1464, 1469, 15 USPQ2d 1525, 1528 (Fed. Cir. 1990)."

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 3, 4, 6, 8-12, 14, 15, 18, 19, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over the American Express Blue card (as taught by "Braving E-Shopping Frontier" from CBS News ("Brave"), "WHAT'S NEXT; New Ways of Securing Online Data" from the New York Times ("Next"), "Going Online? New law means you'll probably should bring along some digital ID" from the San Jose Mercury News ("ID"), "American Express Has New Card With 'Key' For Online Shoppers" from The Wall Street Journal ("WSJ"), and "American Express Blue" from http://www.compukiss.com ("Kiss")) (hereafter "Blue"), in view of the SSL protocol (as taught by Network Security Essentials: Applications and Standards, by William Stallings, hereafter "Stallings"), further in view of Handbook of Applied Cryptography, by Menezes, Alfred et al ("Handbook").

11. As per claims 1 and 12, Blue discloses:

12. first site coupled to a network (Kiss, ¶5 - "I surfed over to Amazon.com");

13. terminal coupled to a network for performing a first portion of a transaction with the first site via the network (Brave, ¶13 - "American Express has a new card…you slide Blue into a little card reader attached to your computer");

14. second site coupled to the network for performing a second portion of the transaction (WSJ, ¶4 - "Once approved by the smart-card reader, the shopper can then use a separate

program to automatically fill in the merchant's online purchase forms") that requires personal data (WSJ, ¶4 - "with the user name and other crucial card information");

15. secure device coupled to the terminal (Brave, ¶13 - "American Express has a new card…you slide Blue into a little card reader attached to your computer"), the secure device containing an encrypted (ID, page 2, ¶9 - "if a Blue card is lost or stolen, the cardholder's personal data becomes available to any hacker who can figure out the secret PIN" - the data on the card is encrypted) version of the personal data and a first key for decrypting the encrypted personal data (Next, page 2, ¶6 - "The thief would have to copy the data stored inside the card…");

16. secure device provides the terminal with the encrypted personal data (Kiss, ¶5 - "all of my credit card and delivery information was transferred automatically". The information is sent from the card, through the smart card reader, to the computer - as the computer is the only device in the chain that can actually send the information over the network).

17. Blue does not explicitly disclose:

18. wherein the second site transmits to the terminal via the network a certificate for verifying the identity of the second site, logic for re-encrypting the decrypted personal data with a second key, logic for transmitting the re-encrypted personal data to the second site via the network, second site having logic for decrypting the re-encrypted personal data and logic for using the personal data to complete the second portion of the transaction, the information identifying certificates that have been revoked or are no longer valid, list containing information

for authenticating the certificate of the second site is transmitted from the first site to the terminal via the network prior to the receipt of the certificate by the terminal;

a. SSL teaches certificates that uniquely identify hosts' identities (Stallings, page 207, "Peer certificate"; page 213, "certificate - Chain of X.509v3 certificates"), encrypting data between two hosts and allowing for its decryption (Stallings, pages 208, 218, "master secret", the master secret being used to encrypt data, as it is shared between both hosts; page 210, "Next, the compressed message plus the MAC are encrypted using symmetric encryption"), and sending encrypted data between two hosts (Stallings, page 218 "At this point the handshake is complete and the client and server may begin to exchange application layer data"). Furthermore, the X.509v3 certificates used in SSL also teach "CRLs", or "Certificate Revocation Lists" (RFC 3280, page 125, section C.4), which informs clients of certificates whose authority to operate as certificates has been revoked. Finally, Digital Certificates have "chains" which identify a higher authority, which in turn identify a higher authority, etc. until a client can authenticate the certificate up to a top authority such as a Certificate Authority (CA). See RFC 3280 generally.

b. SSL is used to enhance web security, and make "use of TCP to provide a reliable end-to-end secure service" (Stallings, page 206).

c. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Blue to use the SSL service as described by SSL, because it would result in a more secure system. A person having ordinary skill in the art would see this as advantageous because it allows for a more trustworthy and secure system, one

that users would be more likely to use because of its increased security and trustworthiness.

19. secure device providing first key to the terminal, terminal having logic for decrypting the encrypted personal data using the first key.

d. Neither Blue, SSL, nor the combination of both references explicitly teach sending encrypted data with a key, and the receiving device decrypting the data using the key, a well-known (to those skilled in the art at the time of the invention) method of sending secure data. Handbook teaches a hybrid encryption protocol, whereby public key cryptography is used to encrypt a private key, and the private key is used to encrypt the data (see page 513, Protocol 12.44). The Beller-Yacobi protocol is even envisioned as being used with "chipcards" such as Blue (page 512, section 12.5.3).

e. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the combined system of Blue and SSL to utilize a hybrid encryption scheme between the reader and the computer, as it would allow for mutual key agreement and authentication, removing the problems of unauthenticated computers. This would create a more secure system, something that a person having ordinary skill in the art would see as advantageous because users would be more liable to trust and use the system.

20. As per claims 3 and 14, Blue discloses as above, and further discloses:

21. communications between terminal and secure device (Handbook, page 513, Protocol 12.44) and terminal and second site are encrypted with one or more symmetric keys (SSL, page 210 - "Next the compressed message plus the MAC are encrypted using symmetric encryption").

22. As per claims 4 and 15, Blue discloses as above, and further discloses:

23. personal data includes at least credit card information (Kiss, ¶5 - "all of my credit card and delivery information…").

24. As per claim 6, Blue discloses as above, and further discloses:

25. transaction comprises a commercial transaction (Kiss, ¶5 - "I chose the book I wanted to buy") and first site comprises an e-commerce site (ibid, "I surfed over to Amazon.com").

26. As per claim 8, Blue discloses as above, and further discloses:

27. second key comprises a public key associated with the second site (page 218, "Both client and server generate a Diffie-Hellman public key…").

28. As per claims 9 and 18, Blue discloses as above, and further discloses:

29. second certificate associated with the terminal is provided to the secure device to authenticate the terminal before the secure device provides the terminal with the encrypted personal data and first key (Handbook, page 513, Protocol 12.44, see especially step 2(c), as well as in 12.46 (2-pass method), B clearly sends $cert_B$ which is B's certificate).

30. As per claims 10 and 19, Blue discloses as above, and further discloses:

31. notification is transmitted from second site to first site via network upon completion of second portion of transaction (inherent in e-commerce applications; also see Kiss, ¶5 - "One nice feature...allows you to see everything that you purchased so you can easily confirm that you have included all the items you wanted to buy").

32. As per claim 11, Blue discloses as above, and further discloses:

33. secure device detachably coupled to terminal (Kiss, ¶4 - "It is a device not much bigger…cables that attach to the serial port and the keyboard port").

34. As per claims 23 and 24, Blue discloses as above, and further discloses:

35. certificate is a digital certificate issued by certificate authority (Stallings, page 207, "Peer certificate"; page 213, "certificate - Chain of X.509v3 certificates" - these certificates are inherently issued by a Certificate Authority. See the RFC 3280 document, page 5 - "A certificate user should review the certificate policy generated by the certification authority (CA) before relying on the authentication or non-repudiation services associated with the public key in a particular certificate").

36. Claims 2 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blue in view of SSL, further in view of Handbook, further in view of Applicant's Admitted Prior Art.

37. As per claims 2 and 13, neither Blue, SSL, Handbook, nor any combination of the three references, explicitly disclose that the secure device includes a special region that, if tampered

with, renders the secure device inoperable and thereby prevents access to the first key. It is Admitted Prior Art (under MPEP §2144.03(C)) that that deactivating circuitry was old and well-known in the art because it allows for a way to keep private information secure to even the most determined attackers. It was old and well-known to those skilled in the art at the time of the invention to destroy information when the information was important and there was a significant impetus to keep it from being released. This solution provides a more secure system where data will not fall into an attacker's hands.

38. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ a mechanism to destroy circuitry upon an intrusion detection, because it would provide a more secure system where the first key would not be obtained. A person having ordinary skill in the art would understand this as an advantage, namely that an attacker would not be able to compromise the system because of a single card.

39. Claims 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blue in view of SSL, further in view of Handbook, further in view of Official Notice.

40. As per claims 21 and 22, Blue discloses as above, but does not explicitly disclose the secure device providing the terminal with data prior to and separately from the first key. The Examiner takes Official Notice that providing data before and separately from the key was old and well-known in the art because it allows for a faster system. Providing the key and the data would be faster because the "secure device" is likely a less powerful device than the host computer it is attached to (see, e.g. USB keys, printers, barcode scanners - clearly all less powerful than the machines they are attached to). By sending the key and the data to the host

computer, and allowing the host computer, it results in a faster system because the host computer would be able to decrypt the data faster than the secure device would be able to.

41. Furthermore, the recitation of sending the key separately from the data is merely a rearrangement of steps, and would have been obvious to one of ordinary skill in the art at the time of the invention. See MPEP §2144.04(VI)(C) and *In re Japikse*, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950).

42. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to send the key separately from the data to the host computer in the combined system of Blue, SSL, and Handbook, because it would result in a faster system, and is merely a rearrangement of process steps. A person having ordinary skill in the art would see this as advantageous because it would allow for a faster system, one that users would be more likely to use.

Response to Arguments

43. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

44. As per Applicants' arguments concerning the Official Notices, Applicants' attempt at traversing the Official Notice findings as stated in the previous Office Action (Paragraph No. 23, 24) is inadequate. Adequate traversal is a two step process. First, Applicant(s) must state their traversal on the record. Second, and in accordance with 37 C.F.R. §1.111(b), which requires Applicants to specifically point out the supposed errors in the Office Action, Applicants must

state why the Official Notice statements are not to be considered common knowledge or well known in the art.

45. In this application, while Applicants have clearly met step (1), Applicants have failed step (2) since they have failed to argue why the Official Notice statements are not to be considered common knowledge or well known in the art. Because Applicants' traversal is inadequate, the Official Notice statement(s) are taken to be admitted as prior art. See MPEP §2144.03.

Conclusion

46. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

f. Internet Archive Wayback Machine archive of the American Express website - 3 pages concerning Frequently Asked Questions for the American Express Blue's Smart Chip, Smart Card Reader, and the Online Wallet service. Pages were archived 2000-2001.

47. **Examiner's Note:** Although Examiner has cited particular columns, line numbers and figures in the references as applied to the claims above for the convenience of the applicant(s), the specified citations are merely representative of the teaching of the prior art that are applied to specific limitations within the individual claim and other passages and figures may apply as well. It is respectfully requested that the applicant(s), in preparing the response, fully consider the items of evidence in their entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Furthermore, it must be noted that the documents cited on any enclosed PTO-892 or PTO-1449 form are cited in their entirety.

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is (571)270-3462. The examiner can normally be reached on Monday - Friday, 9 am to 5 pm.

49. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

50. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher C Johns
Examiner
Art Unit 3621

CCJ

/ANDREW J. FISCHER/
Supervisory Patent Examiner, Art Unit 3621